Ransomware Mitigation Strategies for Windows Systems: Securing Servers and Endpoints

Carl Lochstampfor Jr.

Department of Cybersecurity, Old Dominion University,

CYSE 280 - Windows Systems Management and Security, Professor Malik A. Gladden

July 31, 2025

Ransomware Mitigation Strategies for Windows Systems

Ransomware is a malicious software that encrypts essential or critical data on Windows servers and endpoints, then demands cryptocurrency ransom payments for decryption keys. When effective, ransomware leaves a trail of destruction and mayhem, causing immense financial and operational chaos for organizations. In 2017, WannaCry crippled over 300,000 computers across 150 countries, including the UK's National Health Service, which lost tens of thousands of dollars each hour while data remained inaccessible. In 2024, a ransomware-as-a-service (RaaS) group named Blackbyte attacked thousands of networks and computers by exploiting unpatched Windows system vulnerabilities and unpatched servers worldwide (Nutland et al., 2024; KL, 2025). In this paper, we examine ransomware mitigation strategies for Windows systems, incorporating technical controls, server management tasks such as patch deployment, and user training to combat phishing tactics (which is one of the most common and successful tactics used in ransomware attacks). Centering on Windows Server (2016/2019/2022) and endpoint (Windows 10, 11) security, we will review and use the BlackByte (2024) and WannaCry (2017) case studies to recommend practical defenses, drawing on scholarly and industry literature. Finally, this paper contains descriptions of ransomware, a review of the ransomware lifecycle, mitigation recommendations, tools, and best practices for defending against ransomware used in proactive data defense.

Overview: What is Ransomware and How Does it Generally Work?

Ransomware often locks down systems and data to varying degrees with its encryption. After encrypting, attackers demand payment of ransoms over digital currencies for the decryption key (see Appendix A: WannaCry Ransom Note). Others, such as hacktivists or even state actors, may also pose a threat of data exfiltration and exposure of sensitive information to the public, where they hold data hostage. Attackers use digital currencies and layer money laundering (e.g., Bitcoin) for anti-forensics evasion of law enforcement's tracking and to realize secure payments.

There are two types or categories of ransomware (Kumar et al., 2020; Kara et al., 2022; McDonald et al., 2022):

- **Crypto Ransomware** (also called Data Locker) renders user data inaccessible by encrypting specific files using strong cryptography, while leaving the machine otherwise operational. This type of ransomware usually demands payment in cryptocurrencies, as victims can still access the internet to facilitate payment.
- **Locker Ransomware** (also known as Computer Locker) denies access to the entire computer or device, often deploying scareware tactics (e.g., fake law enforcement warnings) to pressure victims into paying a ransom. Victims are typically unable to access online payment methods on the locked system.

The cybersecurity community generally advises **AGAINST paying** the ransom. Reasons include (1) attackers may not provide the key, (2) may lack the technical ability to retrieve the key, or (3) paying may fund future malicious activities that harm others. However, many individuals and organizations still pay out the money (Sophos, 2025). Victims often conduct a cost-benefit analysis, finding that the cost of downtime — sometimes thousands or millions of dollars per minute of downed operations — far outweighs the cost of the ransom demand. Furthermore, many victims do not have good data backups or have no reliable way of recovering their data, except for making immediate payment to the extortionists. From the victims' perspectives, paying the attackers seems easier and faster than attempting to get the data decrypted using self-help guides or third-party vendors. However, even with possession of the attacker's decryption key, the decryption process is usually lengthy and there is no guarantee the data will be decrypted and completely accessible. Fortunately, in most cases when the attackers promise to provide a working decryption key to their victims for financial gains, they usually do because their RaaS business model of exhorting people depends on the trust of their victims and the public. Without the public's trust and the attackers' follow-through to fulfill their promises, no victim would pay the monetary ransomware demands and the victims would either accept the situation as a loss or push forward to other Said alternatives and solutions.

Therefore, solid data protection is essential, and fortunately, good backup and data protection services are now more prevalent and easily accessible through the Cloud. Additionally, users should avoid encrypting their backups to simplify the process and not cause additional confusion or headaches. This is why offline, off-premises, 'airgap', and immutable backups are so crucial for preserving data (Messer, 2022; Sandbu, 2022; Hristev and colleagues, 2023). While ransomware groups may also utilize RaaS models to exploit vulnerabilities at institutional levels and generate financial gains, other cybercriminals may be hacktivists or state actors who seek to inflict as much harm as possible on victims by refusing to decrypt data (Sandbu, 2022; Hristev et al., 2023).

Given that ransomware has been a long-standing threat to digital organizations, primarily targeting Windows systems, organizations need to focus on server and endpoint attacks with a well-designed defense (Sandbu, 2022). An effective defense requires individuals and organizations to understand the ransomware lifecycle (see Appendix B: Ransomware Lifecycle) and implement comprehensive mitigation strategies that focus on both server and endpoint security (Sandbu, 2022).

1. **Infection:** Attackers target victims using phishing emails, malicious attachments, or software exploits to infiltrate and infect systems. Phishing and social engineering are standard methods to trick users into installing or clicking malware on their own devices

(Verizon Business, 2024; Sophos, 2025). Additionally, attackers can also exploit system inherent or zero-day vulnerabilities without requiring user interaction, such as the EternalBlue SMB exploit used in WannaCry's 2017 attack on unpatched Windows systems (Kumar et al., 2020; Connolly & Wall, 2021).

2. **Propagation:** Once infection is established, ransomware spreads via network vulnerabilities or Remote Desktop Protocol (RDP), such as in BlackByte's 2024 server attacks. In contrast to WannaCry's worm-like spread that occurs without user interaction, BlackByte may often use stolen credentials scraped from already infected systems to gain lateral movement and privileged access within networks (Kumar et al., 2020; Nutland et al., 2024; KL, 2025).
3. **Execution:** Ransomware encrypts files and/or systems using strong algorithms, such as AES-256, and displays ransom demands requiring payment in cryptocurrencies. WannaCry, for example, demanded $300–$600 Bitcoin payments. Ransomware also commonly deletes shadow copies using tools like vssadmin.exe to hinder recovery (Kumar et al., 2020).
4. **Impact:** The results are devastating, even catastrophic, as they interfere with business operations and cause financial ruin for individuals and companies. WannaCry was estimated to cost between $4 billion and $8 billion as it brought large institutions, such as the U.K.’s National Health Service, FedEx, Hitachi, Deutsche Bahn, and Boeing, to their knees. Furthermore, BlackByte crippled the servers of numerous companies, incurring millions of dollars in expenses (Kaspersky, 2020; McDonald et al., 2020; KL, 2025).
5. **Mitigation and Recovery:** Deploying patches via Windows Server Update Services (WSUS), using Windows Defender for real-time protection, and restoring data with the 3-

2-1 backups (three copies, two media, one offsite) (Kara, 2022; Messer, 2022; Hristev et al., 2023). In WannaCry, a distinctive kill switch was implemented to stop its propagation; however, complete backups were still essential for organizations to recover data (KL, 2025).

Finally, Windows system vulnerabilities (i.e., unpatched systems, SMB vulnerabilities, susceptibility to phishing) contribute to the widespread execution of ransomware by enabling a variety of exploitable attack vectors. Companies can reduce human error by increasing the effectiveness of user training (i.e., phishing campaigns and simulations), which is a massive source of ransomware infections and network penetrations (Connolly & Wall, 2021).

Mitigation Frameworks and Methodology

On Windows systems, to prevent and recover from ransomware incidents, references to frameworks and an organized process present a structured approach, from prevention to detection and response (See Appendix C and D Flowcharts). The NIST Cybersecurity Framework (NIST SP 1800-26) conceptualizes a holistic framework using five fundamental functional areas: Identify (assets), Protect (proactive controls), Detect (logs), Respond (isolation), and Recover (backups) (Cichonski et al., 2012; Nieles et al., 2017; Cawthra & Colbroth, 2020).

1. **Identify:** This function enables organizations to catalog critical assets, including Windows Server 2016/2019/2022 servers and Windows 10 and 11 endpoints, to help prioritize protection efforts.
2. **Protect:** This function uses technical controls like Windows Defender's Controlled Folder Access to prevent unauthorized file updates. Moreover, WSUS schedules up-to-date patches (e.g., the MS17-010 patch to resolve the WannaCry vulnerability that exploited the

EternalBlue vulnerability) and enforces security policy with Group Policy Objects, such as disabling macros. A hybrid of Application Whitelisting and Blacklisting (e.g., AppLocker, SecureAPlus, VoodooShield) is important in mitigating against zero-day threats, such as those who are unfamiliar with both Windows and AV vulnerabilities are exploited to run malicious code (Turaev et al., 2022; Kumar et al., 2020). Although both Application Whitelisting and Blacklisting work well for zero-day risks, whitelisting introduces management problems, as the process of creating and updating lists of trusted applications can be labor-intensive, especially for large organizations. This is due to forged certificate publishers and user distraction caused by frequent requests.

3. **Detect:** This function uses Event Logs for static and dynamic monitoring for detecting outliers in behavior (e.g., failed logins or suspicious network activity) (Chen et al., 2017; Kara et al., 2022; Sandbu, 2022). Event Logs assist with tagging RDP intrusions and unauthorized lateral movement, which are popular methods for ransomware attacks (Connolly & Wall, 2021).
4. **Respond:** This function includes quarantining infected systems, often leveraging Defender’s automated response capabilities (McDonald et al., 2022).
5. **Recover:** This is based on the 3-2-1 backup rule: three copies of the data, two media types, one offsite — to allow for data recovery without payment of ransoms (Messer, 2022; Sandbu, 2022; Hristev et al., 2023).

Finally, user training complements these technical controls, with phishing simulations for company employees significantly reducing human errors (Nobles, 2018; Verizon Business, 2024; Sophos, 2025). Regular practice, as outlined in CompTIA Security+ and NIST's Data Integrity and Computer Security Incident Handling Guides (Cichonski, 2012; Cawthra et al., 2020), helps users identify and avoid falling prey to phishing attacks. With NIST and Windows-specific processes working together, one can rest assured their organization will be in good hands. In contrast, problems such as zero-day attacks require continual monitoring through a combination of static analysis, dynamic analysis, anomaly detection, and polymorphic behavior detection, as well as Whitelisting and Blacklisting of applications (Chen et al., 2017; Kumar et al., 2020; Turaev et al., 2022).

Tools and Resources

A comprehensive set of tools and resources for technical countermeasures to mitigate ransomware in Windows systems is necessary, which are validated using case studies such as BlackByte (2024) and NSK, as with WannaCry (2017).

- **Windows Defender:** The OS's built-in antivirus provides real-time protection and Controlled Folder Access, critical for preventing unauthorized file encryption on both servers and endpoints (Sandbu, 2020).
- **Microsoft's AppLocker:** Restricts unauthorized software execution, blocking malicious payloads (e.g., BlackByte) from auto-executing on user operating systems (Turaev et al., 2022).
- **Windows Server Update Services (WSUS):** Delivers patches (e.g., MS17-010) to close system vulnerabilities, such as WannaCry's EternalBlue SMB flaw (Kaspersky, 2020; Kumar et al., 2020).
- **Group Policy Objects (GPOs):** Enforce security policies, including disabling macros and strengthening server passwords to counter attacks like BlackByte's RDP incursions (McDonald et al., 2022).

- **Event Logs:** Monitor attack indicators—such as failed logins, critical file modifications, disabled security software, and unusual disk/memory activity—to enable early detection and containment (Connolly & Wall, 2021; Kara et al., 2022).
- **Backups:** Following the 3-2-1 rule (three copies, two media, one offsite) ensures data recovery (Messer, 2022; Sandbu, 2022; Hristev et al., 2023).
- **User Training:** Particularly phishing simulations, addresses human vulnerabilities (Nobles, 2018).

Table 1:
Tools and Resources Chart

Tool	Functionality	Ransomware Mitigation Impact	Complexity
Windows Defender	Real-time protection, Controlled Folder Access	Blocks encryption	Low
AppLocker	Restricts unauthorized software	Prevents payload execution	Medium
WSUS	Delivers security patches	Closes vulnerabilities	Medium
GPOs	Enforces security policies	Secures systems	Medium
Event Logs	Monitors attack indicators	Enables early detection	Medium
Backups	3-2-1 backup strategy	Ensures data recovery	Medium
User Training	Phishing simulations	Reduces infection risks	Low

Case Study Results

- **BlackByte (2024):** This RaaS group targeted Windows servers by exploiting unpatched VMware ESXi servers (CVE-2024-37085) and RDP using stolen credentials, to exfiltrate data with tools like ExByte. Mitigation included enabling/updating Windows Defender's real-time protection, implementing/updating GPOs for secure configurations, and creating 3-2-1 backups.

- **WannaCry (2017):** Infected over 300,000 systems worldwide via the EternalBlue SMB vulnerability (CVE-2017-0144) while demanding Bitcoin for ransom payment to decrypt data. WSUS patches (MS17-010), Defender updates, and a unique kill switch halted its spread, with backups enabling swift recovery. Kumar et al. (2020) detail WannaCry's execution process, which included the mssecsvc.exe and tasksche.exe components, as well as the deletion of shadow copies to hinder recovery. McDonald et al. (2022) revealed that WannaCry, along with other variants, did not stop critical Active Directory services (e.g., Logon, DNS, DHCP, IIS) but rendered them dysfunctional by encrypting associated files; for instance, while IIS remained online, referenced image files were encrypted, causing web pages to display incorrectly.

Table 2:
Case Study Results

Attack	Attack Vector	Tools Used	Outcome
BlackByte (2024)	RDP, unpatched servers (CVE-2024-37085)	Defender, GPOs, backups	Partial recovery
WannaCry (2017)	EternalBlue SMB exploit	WSUS, Defender, kill switch	Spread halted

Conclusion

Ransomware remains a dangerous threat to Windows systems worldwide. However, as seen in the BlackByte (2024) and WannaCry (2017) case studies, Windows OS users have a wide array of strategies and tools to combat ransomware. Options including Windows Defender, AppLocker, WSUS, GPOs, Event Logs, and backups, combined with user training, offer effective mitigation. Defender's real-time protection and AppLocker's software restrictions prevent malware execution. WSUS patches critical OS vulnerabilities, such as WannaCry's SMB exploit (Kumar et al., 2020). GPOs enforce secure configurations, and Event Logs enable early detection, critical for BlackByte's RDP attacks (McDonald et al., 2022; Kara et al., 2022). The 3-2-1 backup strategy ensures recovery without ransom payment (Messer, 2022; Hristev et al., 2023). Phishing campaigns or simulations aim to enhance human cognition by improving the understanding, identification, detection, and avoidance of malicious content, thereby reducing human errors that drive ~90% of attacks. (Connolly & Wall, 2021; Sandbu, 2022; Verizon Business, 2024; Sophos, 2025). However, zero-day exploits and user non-compliance continue to pose ongoing challenges, necessitating proactive measures to address these issues.

Recommendations

The following list of recommendations are essential to the strategic building and security of organizations (KL, 2025). They align and comply with NIST's Protect-Recover model and modern guidelines (Nieles et al., 2017; Cawthra et al., 2020).

- **Backups:** Conduct monthly testing of the 3-2-1 backup strategy to ensure data integrity and reliability. Maintain password-protected, offline, off-premises, and immutable backups of critical data in a safe and secure environment to prevent encryption of backups (Messer, 2022; Sandbu, 2022; Hristev et al., 2023).
- **Incident Response Team:** Develop and regularly test comprehensive incident response plans to ensure swift and effective response to potential cyber-attack threats (Nobles, 2018; Connolly & Wall, 2021; Kara et al., 2022; Microsoft Incident Response, 2023).
- **EDR Solution:** Implement an Endpoint Detection and Response (EDR) solution (e.g., Microsoft Defender for Endpoint) to detect and respond to malicious behavior on endpoints (Sandbu, 2020; Microsoft Incident Response, 2023).

- **Tamper Protection (Software and Hardware):** Enable tamper protection to prevent disabling critical security software and unauthorized physical adjustments to hardware components, including the insertion of malicious USB devices (Microsoft Incident Response, 2023; KL, 2025).
- **WSUS Management:** Deploy WSUS patches within 48 hours to close vulnerabilities promptly (Connolly & Wall, 2021; Kara et al., 2022; Microsoft Incident Response, 2023).
- **Authentication and Authorization:** Configure GPOs to disable macros, enforce strong passwords, and implement Multi-Factor Authentication (MFA) for all remote access devices. Utilize the principle of Least Privilege and Role-Based Access Controls (RBACs) to limit administrative and user privileges based on need-to-know access (Sandbu, 2020; Connolly & Wall, 2021; McDonald et al., 2022).
- **Employee Training & Human Factors Integration:** Conduct quarterly phishing simulations and incentivize participation and reporting throughout the year to reduce infection risks. Beyond training, integrate human factors objectives into security strategy and establish executive-led committees to address human-enabled errors. Foster a culture recognizing that human errors, often unintentional due to workload or time pressure, account for the majority of cyber incidents, requiring interdisciplinary approaches from behavioral science experts (Nobles, 2018; Connolly & Wall, 2021; Kara et al., 2022).
- **Network Segmentation:** Isolate critical systems and limit lateral movement within the network (Sandbu, 2020; Connolly & Wall, 2021).
- **Threat Intelligence:** Utilize feeds and platforms to stay informed about the latest malicious threats (Connolly & Wall, 2021; Kara et al., 2022).

- **SMB Protocol Security:** Disable SMBv1 and enforce SMB signing and encryption (Kumar et al., 2020; McDonald et al., 2022).
- **Account Commissioning and Decommissioning:** Develop and regularly review procedures for managing accounts. Periodically review existing accounts to disable those of inactive users, such as those of discontinued vendors or former employees.
- **Future Actions:** Continuously monitor ransomware-as-a-service (RaaS) trends (e.g., BlackByte) and media news for relevant updates (CISA Known Exploited Vulnerabilities (KEV) Catalog (cisa.gov); National Vulnerability Database (NVD) (nvd.nist.gov); SecurityWeek (securityweek.com)), update Defender signatures weekly, and audit Event Logs to detect anomalies (Microsoft Incident Response, 2023; Verizon Business, 2024; Sophos, 2025).

References

Cawthra, J., Ekstrom, M., Lusty, L., & Sexton, J., & Sweetnam, J. (2020, December). *Data integrity: Detecting and responding to ransomware and other destructive events* (NIST SP 1800-26B, Vol. B: Approach, architecture, and security characteristics) [Cybersecurity practice guide]. National Cybersecurity Center of Excellence, National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.1800-26

Chen, Qian, & Bridges, Robert A. (2017). *Automated behavioral analysis of malware: A case study of WannaCry ransomware*. In X. Chen, B. Luo, F. Luo, V. Palade, & M. A. Wani (Eds.), Proceedings of the 16th IEEE International Conference on Machine Learning and Applications (ICMLA 2017) (pp. 454–460). Institute of Electrical and Electronics Engineers Inc. https://ieeexplore.ieee.org/document/8260673

Cichonski, P. R., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer security incident handling guide* (NIST Special Publication 800-61 Rev. 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2

Connolly, L. Y., & Wall, D. S. (2021). *The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures*. Computers & Security, 108, 102345. https://www.sciencedirect.com/science/article/pii/S0167404819301336

Hristev, R., Veselinova, M., & Kolev, K. (2023). *Ransomware attacks on Windows servers: Infection and recovery*. Electronics, 12(4), 789. https://www.researchgate.net/publication/375282292_RANSOMWARE_ATTACKS_ON_WINDOWS_SERVERS_INFECTION_AND_RECOVERY

Kara, I., & Aydos, M. (2022). *The rise of ransomware: Forensic analysis for Windows based ransomware attacks*. Expert Systems With Applications, 190, 116198. https://www.sciencedirect.com/science/article/pii/S0957417421015141

Kaspersky. (n.d.). (2020, April 20). *Ransomware WannaCry: All you need to know*. Kaspersky. Retrieved July 19, 2025, from https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

KL, Arun. (2025, March 17). *BlackByte ransomware: Analysis & defense guide*. TheSecMaster. https://thesecmaster.com/blog/blackbyte-ransomware

Kumar, R., Ben-Othman, J., & Srinivasagan, K. G. (2020). *An investigation on WannaCry ransomware and its detection*. Electronics, 9(8), 1312. https://ieeexplore.ieee.org/document/8538354

McDonald, G., Papadopoulos, P., Pitropakis, N., Ahmad, J., & Buchanan, W. J. (2022). *Ransomware: Analysing the impact on Windows Active Directory domain services*. Sensors, 22(3), 953. https://www.researchgate.net/publication/358119298_Ransomware_Analysing_the_Impact_on_Windows_Active_Directory_Domain_Services

Microsoft Security Blog: Microsoft Incident Response. (2023, July 6). *The five-day job: A BlackByte ransomware intrusion case study*. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2023/07/06/the-five-day-job-a-blackbyte-ransomware-intrusion-case-study/

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). *An introduction to information security* (NIST Special Publication 800-12, Revision 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-12r1; https://csrc.nist.gov/pubs/sp/800/12/r1/final

Nobles, C. (2018). *Botching human factors in cybersecurity in business organizations*. HOLISTICA, 9(3), 71–88. https://www.researchgate.net/publication/329806166_Botching_Human_Factors_in_Cybersecurity_in_Business_Organizations

Nutland, J., Jackson, C., Valikodath, T., & Evans, B. (2024, August 28). *BlackByte ransomware exploits VMware ESXi flaw in latest attack wave*. The Hacker News. https://thehackernews.com/2024/08/blackbyte-ransomware-exploits-vmware.html

Professor Messer. (2022). *Managing Backups – CompTIA A+ 220-1102 – 4.3* [Video]. Retrieved July 19, 2025, from https://www.professormesser.com/free-a-plus-training/220-1102/220-1102-video/managing-backups-220-1102/

Sandbu, M. (2022). *Windows ransomware detection and protection*. Packt Publishing.

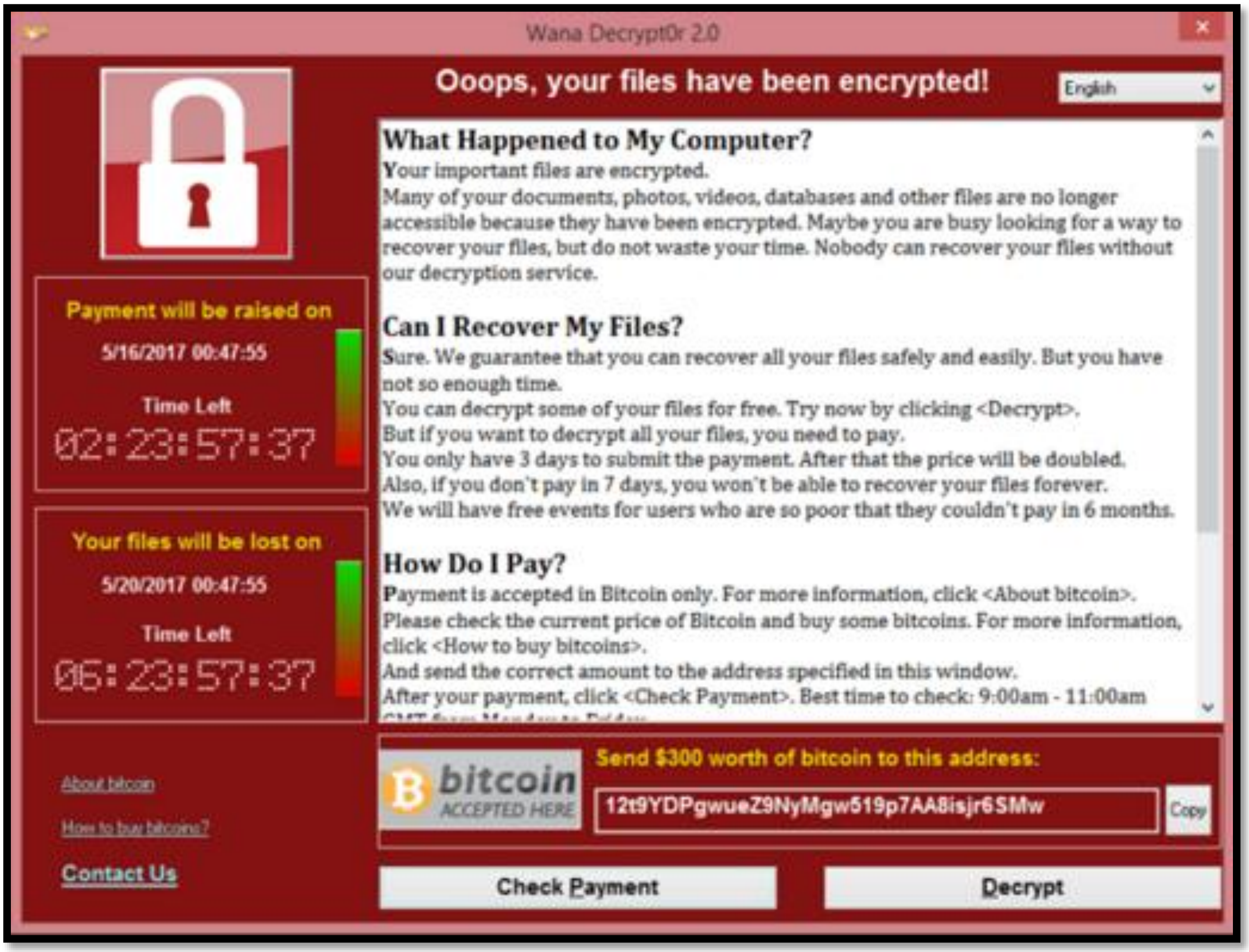
Sophos. (2025, June). *The state of ransomware 2025* [White paper]. Sophos. Retrieved July 19, 2025, from https://assets.sophos.com/X24WTUEQ/at/9brgj5n44hqvgsp5f5bqcps/sophos-state-of-ransomware-2025.pdf

Turaev, H., Zavarsky, P., & Swar, B. (2022). *Prevention of ransomware execution in enterprise environment on Windows OS: Assessment of application whitelisting solutions*. Journal of Cybersecurity, 8(1), tyac012. https://ieeexplore.ieee.org/document/8367748

Verizon Business. (2024, June). *2024 Data Breach Investigations Report*. Retrieved July 23, 2025, from https://www.verizon.com/business/resources/reports/dbir/#top-takeaways

Wikipedia. (n.d.). (2017, May 13). *WannaCry ransomware attack*. Retrieved July 18, 2025, from https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

Appendix A:
WannaCry Ransom Note (Wikipedia, 2017)



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

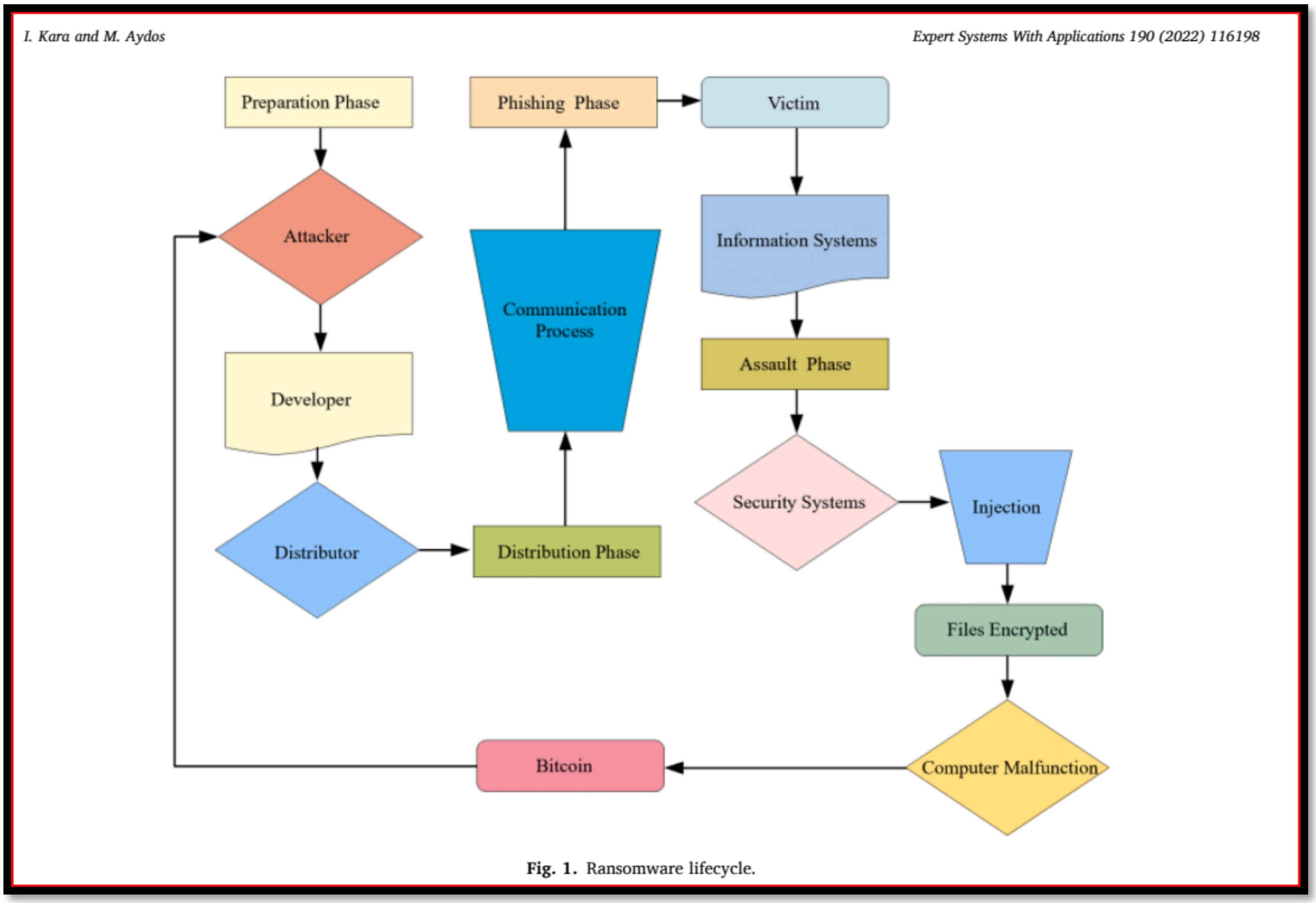
And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Appendix B:
Ransomware Lifecycle (Kara et al., 2022)

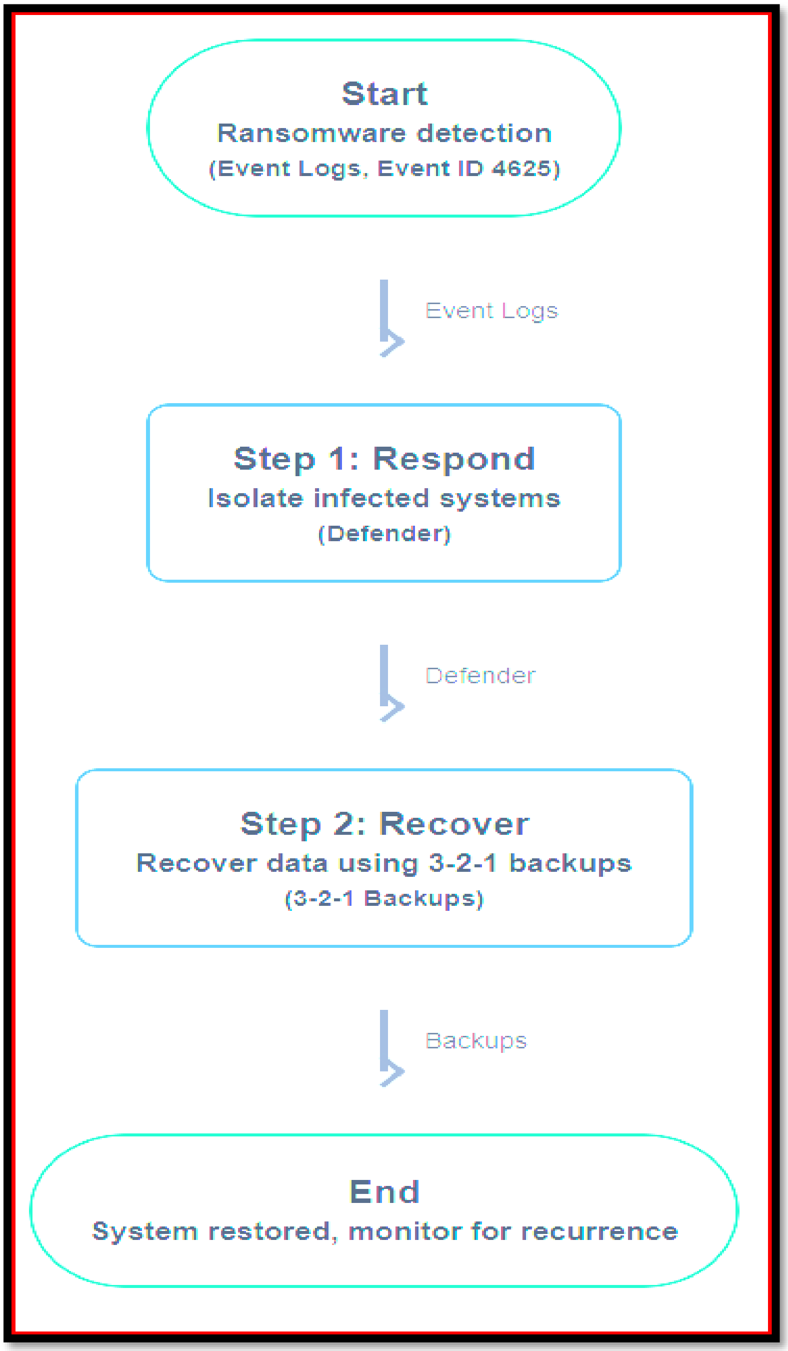


I. Kara and M. Aydos

Expert Systems With Applications 190 (2022) 116198

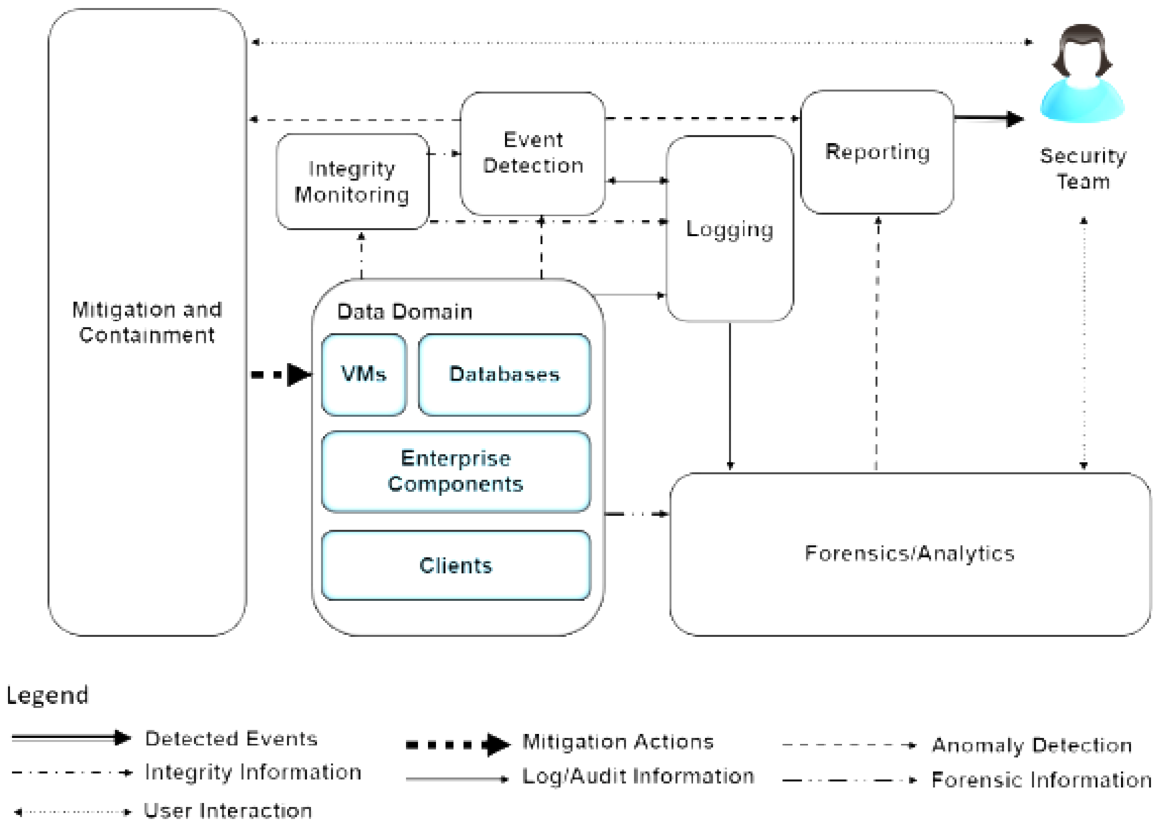
Fig. 1. Ransomware lifecycle.

Appendix C, Flowchart: Mitigation Frameworks and Methodology



Appendix D, Flowchart: Detection and Response Phases (Cawthra et al, 2020)

Figure 4-1 DI Detect & Respond High-Level Architecture


Mitigation and Containment
Integrity Monitoring
Event Detection
Logging
Reporting
Security Team
Data Domain
VMs
Databases
Enterprise Components
Clients
Forensics/Analytics
Legend
Detected Events
Integrity Information
User Interaction
Mitigation Actions
Log/Audit Information
Anomaly Detection
Forensic Information